CUREX – seCUre and pRivate hEalth data eXchange

Prof. Christos Xenakis,
Coordinator of the CUREX Project

University of Piraeus, Greece

3-4 June 2021 (digital) Brussels, Belgium

19th eHealth Network

Participating H2020 Projects

CUREX
SECURE AND PRIVATE HEALTH DATA EXCHANGE

Secure and private
health data exchange

Panacea
People-centric cybersecurity in healthcare

Protection and privacy of hospital and health infrastructures with smart cyber security and cyber threat toolkit for data and people

ProTego

Data-protection toolkit reducing
risks in hospitals and care centers

Funded under the SU-TDS-02-2018 topic for:
Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures

SPHINX

A universal cyber security toolkit
for health-care industry

Projects Information

- **Programme:** Improving health information and better use of health data (H2020-EU.3.1.5.1.)
- **Topic:** Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures (SU-TDS-02-2018)
- **Call:** Trusted digital solutions and Cybersecurity in Health and Care (H2020-SC1-FA-DTS-2018-1)
- **Funding Scheme:** RIA - Research and Innovation action
- **EU contribution per project:** ~ € 5M
- **Duration:** All projects are currently in their third and final year.

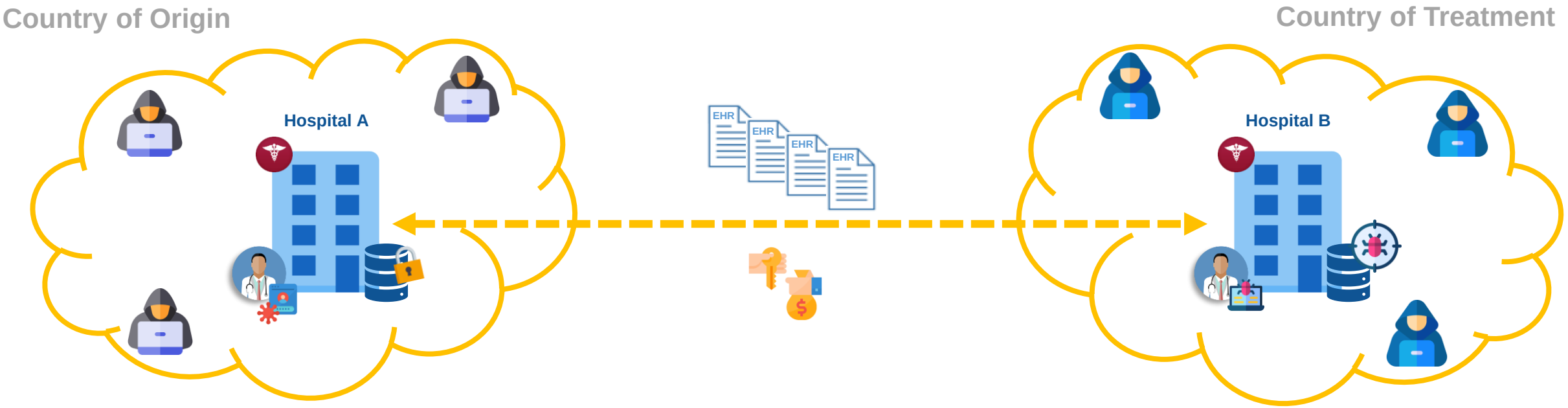
Background

- After the end of the prolonged mobility restrictions, citizens will once again be on the move, free to travel or even relocate as the “work from home” model keeps gaining traction.
  - **Patients’ Rights Directive (2011/24/EU)** foresees that an individual who travels within the EU will receive the same healthcare service as in their home state.
  - **eHDSI** lays out the technical specifications on how it can actually be implemented.
- At the same time, according to reports published by cyber intelligence centres, the healthcare sector suffered in 2020 a substantial increase in the number of reported breaches and incidents.
  - For healthcare systems to become interconnected and interoperable, additional end-points are required, **increasing the attack surface**.
  - Substantial effort has been invested by the **EU to enhance cybersecurity** for all member states (e.g., NIS Directive).
  - **eHDSI** has also considered cybersecurity.
- How can EU-funded research contribute?

Cybersecurity for cross-border healthcare

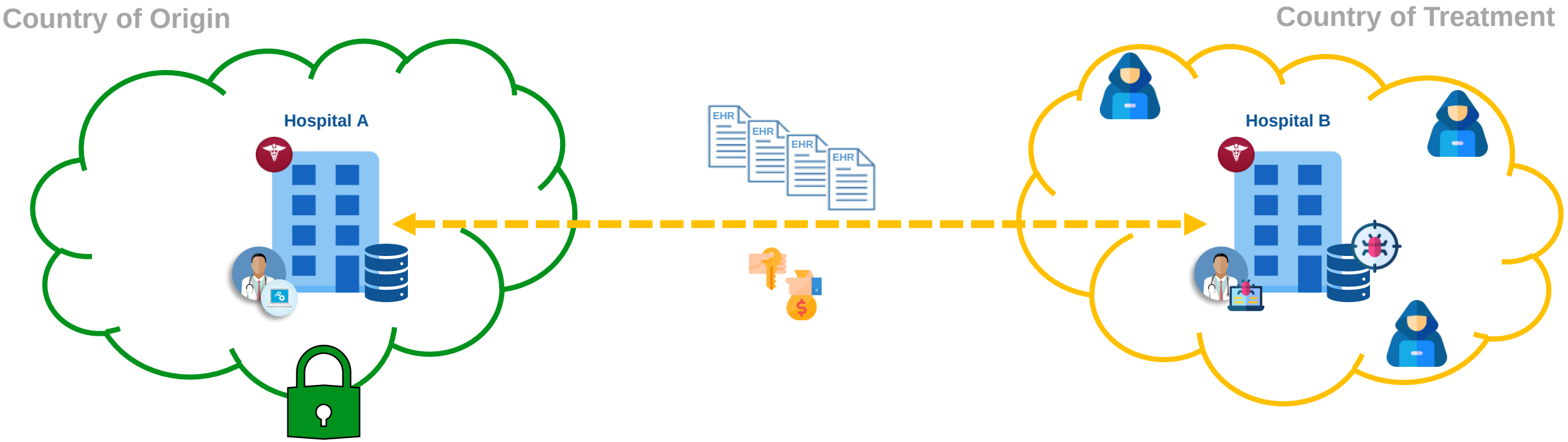
A robust framework for **Health Information Exchange** is the only way to enable **continuity of care** across Europe.

Cybersecurity for cross-border healthcare



A robust framework for **Health Information Exchange** is the only way to enable **continuity of care** across Europe.

Cybersecurity for cross-border healthcare

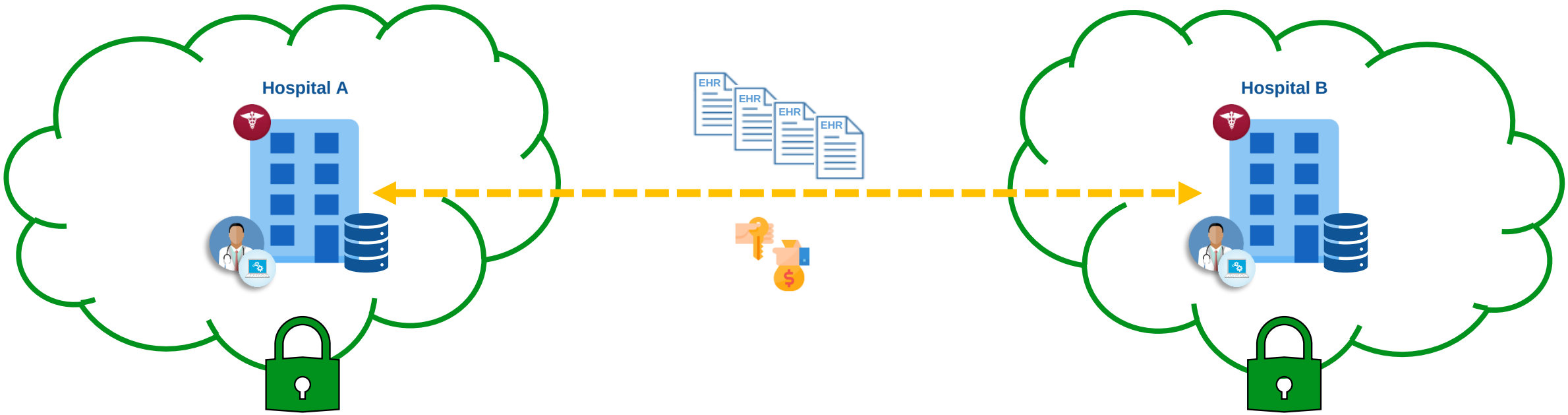


A robust framework for **Health Information Exchange** is the only way to enable **continuity of care** across Europe.

Cybersecurity for cross-border healthcare

Country of Origin

Country of Treatment



A robust framework for **Health Information Exchange** is the only way to enable **continuity of care** across Europe.

Cybersecurity for cross-border healthcare

A robust **and secure** framework for **Health Information Exchange** is the only way to enable **continuity of care** across Europe.

CUREX
SECURE AND PRIVATE HEALTH DATA EXCHANGE

Project Details

Aim

CUREX aims to protect the health data handled by hospitals from the risks that are propagated all the way from the security gaps in their IT infrastructure.

How

- By performing cybersecurity and privacy risk assessments.
- By offering optimal recommendations for cyber risk mitigation in the form of a decision support too.
- By leveraging the blockchain technology to provide accountability and auditability for data transactions, building trust.
- By improving the cyber hygiene culture among personnel.

Pilots

- Hospital Universitario Puerta de Hierro Majadahonda, Spain
- Fundación Privada Hospital Asil de Granollers, Spain
- Karolinska Institutet, Sweden

Funding

CUREX has received € 4 987 825 from European Union's Horizon 2020 research and innovation programme under grant agreement No 826404.

Consortium

17 participants from 9 EU countries

- 7 x research institutes and universities
- 2 x healthcare representatives
- 2 x large industries
- 6 x SMEs

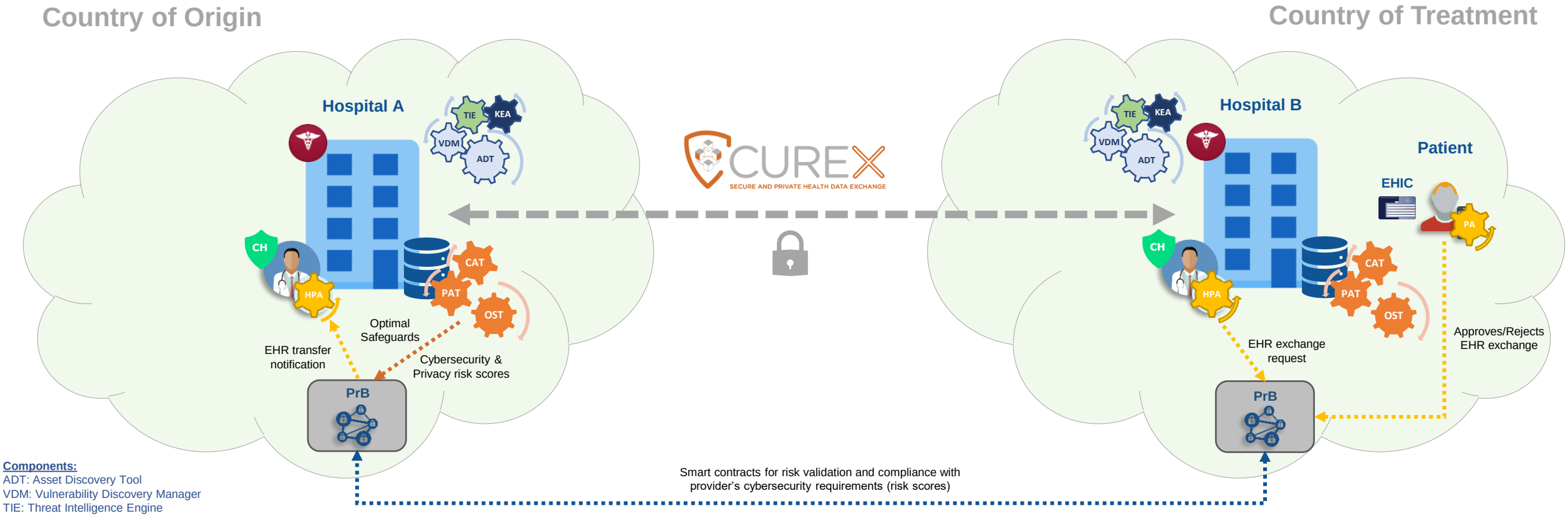
Dates

- Start Date: December 1st, 2018
- End date: November 30th, 2021
- Duration: 36 months

www.curex-project.eu
info@curex-project.eu
CUREX Project
CUREXH2020
CUREX_H2020
CUREXH2020

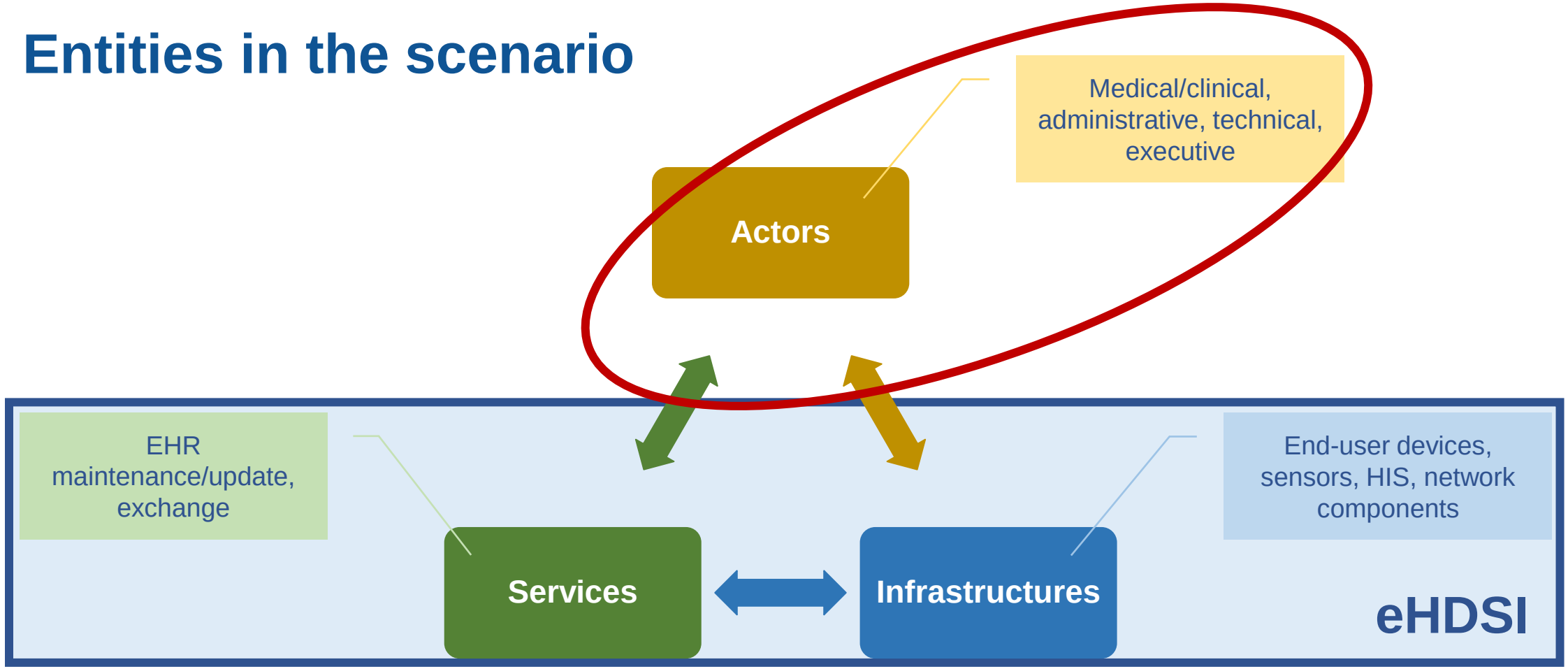
CUREX's take on cross-border healthcare security

Use Case 1 – Data exchange for cross-border patient mobility: Emergency in a foreign country



Components:
ADT: Asset Discovery Tool
VDM: Vulnerability Discovery Manager
TIE: Threat Intelligence Engine
KEA: Knowledge Extraction Analytics
CAT: Cybersecurity Assessment Tool
PAT: Privacy Assessment Tool
OST: Optimal safeguards Tool
PrB: Private Blockchain
CH: Cyber Hygiene

Entities in the scenario



Actors

- Services and Infrastructures are **operated by different types of personnel**.
  - But the human factor is often neglected in the chain of cyber defence.

- A healthcare organisation employs people with **diverse backgrounds, level of experience, and expertise**.
  - An employee may use, manage, or make decisions that affect different critical operations on a daily basis.
  - Educating employees on how to safely interact with the organisations' systems and procedures has become mandatory.

- However, employees coming from **different fields do not exhibit similar knowledge gaps** with regards to cybersecurity and data privacy.
  - For example, while some may understand the technical aspects of cybersecurity, they may lack knowledge regarding the applicable regulatory framework.
  - Training frameworks cannot be "one-size-fits-all".

Actions taken by CUREX

- CUREX aims to promote **Cyber Hygiene** through the identification of strategies for **addressing risks related to cybersecurity and data privacy awareness of different employee groups** in a healthcare organization.

- Highlights of the proposed solution for Cyber Hygiene
  - Survey-based **risk assessment** methodology for improving Cyber Hygiene
  - Reveals **risks** related to various aspects of Cyber Hygiene
  - Recommends **human-centric** controls (i.e., actions, interventions) to **mitigate** risks
  - Supports the **management** team in cyber defence **decision-making**

Outline of the Methodology

1. Extract knowledge and assess the needs and gaps of different employee groups at healthcare organisations through a **survey** questionnaire.
2. Process and analyse the participants' **responses.**
3. Identify the most effective **strategy** to address each cybersecurity and data privacy risk.
4. Recommend targeted human-centric **controls** to implement the strategy.
5. The management team can apply the controls to the **workforce** to improve the situation.

The Methodology in a nutshell

- 4 employee groups
  - Administrative; Medical/Clinical; IT/Technical; Executive/Security
- 7 Risk Categories
  - Risk quantification based on collected responses from a survey questionnaire
- 5 Risk Strategies
  - Mitigation (high risk) → Acceptance (low risk)
- 19 human-centric Controls
  - Developed in CUREX and inspired by CIS Control 17* and PANACEA project
  - Related to **Training**, **Awareness**, **Motivation** and **Rewarding**
  - Implementation levels: **Frequency** (weekly, monthly, etc.), **Content** (Beginners, etc.)
- Mapping of Controls to Strategies

*CIS Control 17: Implement a Security Awareness and Training Program (CIS Controls V7.1)

Linking with CUREX Use Case 1 – Cross-border patient mobility

- Target group: Medical/Clinical personnel using the Health Professional Application (HPA)

Related Risk Categories	Risk description
Cyber Hygiene	Not aware of what Cyber Hygiene is
Cybersecurity Awareness	Not aware of cybersecurity threats in healthcare and related incidents
Data Privacy/Protection Awareness	Not aware of what GDPR is, data privacy/protection threats in healthcare and related incidents
Data Privacy/Protection Training	Not attending existing training, not considering data privacy during daily work, not knowing about internal procedures for data privacy threats and who is responsible for data protection, managing personal data frequently, limited knowledge about data privacy (self-assessed)
Secure connection and use of devices	Not aware of or not following policies, guidelines, or best practices about remote connection, using personal devices (BYOD), using public access networks, and using personal USB sticks

If the HPA runs on the doctor's smartphone

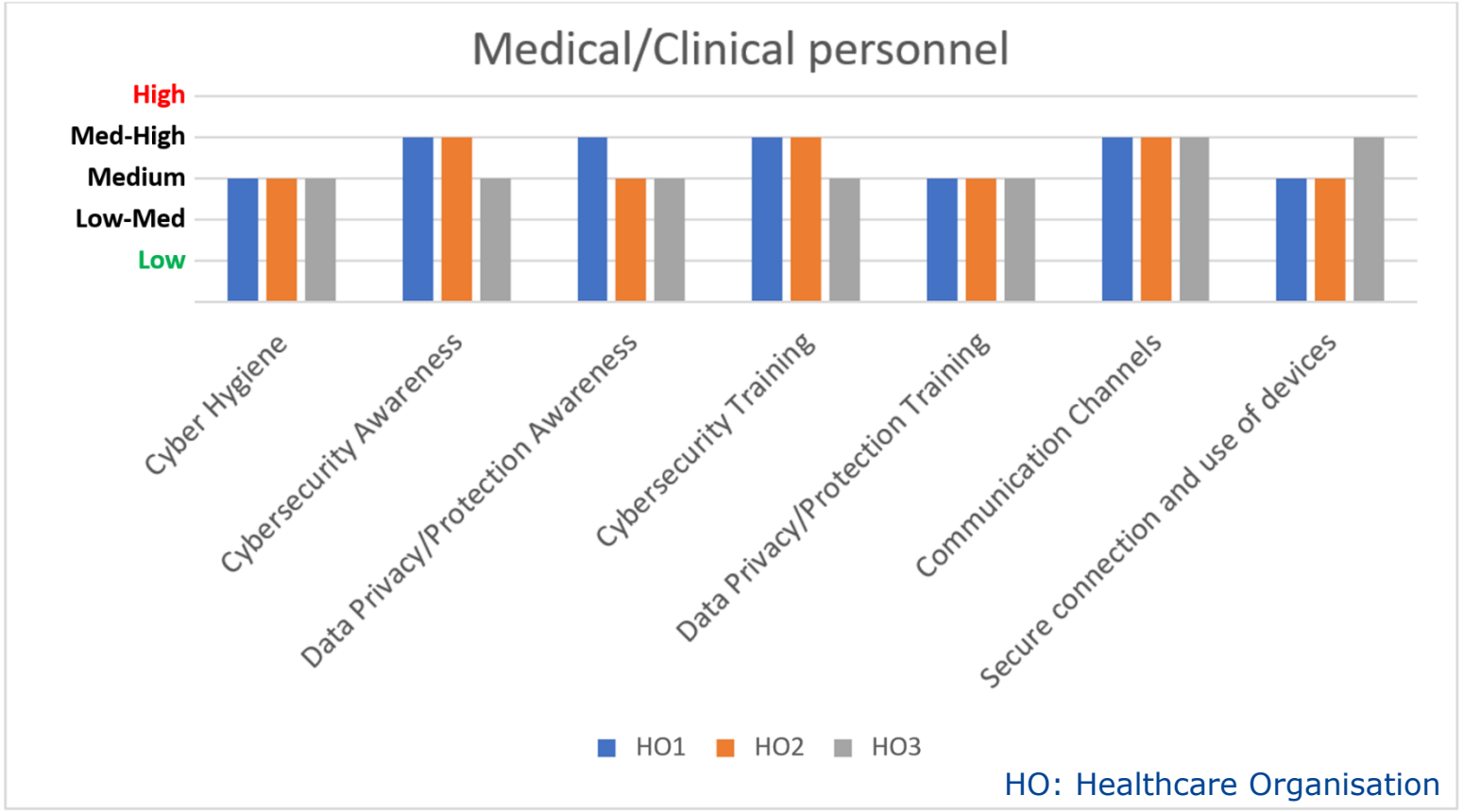
Increased teleworking during the pandemic

Selected related controls

No	Control Title	Control Description
C3	Implement a Cybersecurity Awareness Program	Create a cybersecurity awareness program for employees to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organisation.
C4	Implement a Data Privacy Awareness Program	Create a data privacy awareness program for employees to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organisation.
C6	Train Workforce on Secure Authentication	Train employees on the importance of enabling and utilising secure authentication.
C7	Train Workforce on Identifying Social Engineering Attacks	Train employees on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls.
C10	Train Workforce on Causes of Unintentional Data Exposure	Train employees to be aware of causes for unintentional data exposures, such as losing their mobile devices or a USB stick with sensitive data, emailing the wrong person, etc.
C11	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.
C12	Include Cybersecurity in the meetings' agenda	Set Cybersecurity as a standing agenda item at meetings.

Relevant Findings

- Medium-High risk in HO1 and HO2 on “Cybersecurity Training”
  - **Key controls: C7, C11, C12**
- Medium-High risk in HO3 on “Secure connection and use of devices”
  - **Key controls: C3, C4, C6, C10**



HO: Healthcare Organisation

CUREX
SECURE AND PRIVATE HEALTH DATA EXCHANGE

Potential Relevance to EU Policies

- Problem Statement
  - Healthcare organisations are requested to apply **general** EU cybersecurity and data privacy guidelines that focus on the **human factor** (awareness, training). But these are hard to map to **specific** actions/controls with **measurable** effect on personnel.
- Areas of Improvement
  - **Tools** and structured **methodologies** for assisting the higher management to select the most **effective** actions/controls for each employee group in the organisation.
- Contribution of the Project's Results
  - Recommends **targeted** controls that are tailored to the organisation-specific **needs** (e.g., culture, knowledge background, etc.) and **constraints** (e.g., available budget and time).
  - After applying the controls, another iteration can be performed (e.g., after 2 years) to re-assess the risks through the survey (step #1) and recommend additional controls if needed.

Questions?

Further information

eHealth Network
https://ec.europa.eu/health/ehealth/policy/network_en

All events
https://ec.europa.eu/health/ehealth/events_en#anchor0